



# CVE-2023-0357

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-0357
<b>State</b>	PUBLIC
<b>Assigner</b>	help@fluidattacks.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-04-04 23:15:00 UTC
<b>Updated</b>	2023-04-10 18:17:00 UTC
<b>Description</b>	Helpy version 2.8.0 allows an unauthenticated remote attacker to exploit an XSS stored in the application. This is possible k

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Helpy.io	Helpy	2.8.0	All	All	All

## References

### Reference

- GitHub - helpyio/helpy: Helpy is a modern, open source helpdesk customer support application. Features include knowledgebase, community
- Helpy 2.8.0 - Stored Cross-Site Scripting | Advisories | Fluid Attacks
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)